APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/941,326	08/29/2001	Timothy Roscoe	1589a	6834

28005   7590   05/30/2006

SPRINT
6391 SPRINT PARKWAY
KSOPHT0101-Z2100
OVERLAND PARK, KS 66251-2100

EXAMINER
POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 05/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/941,326	ROSCOE ET AL.
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3/07/06*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24,26-28,30-38,42-45 and 50-53* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24,26-28,30-38,42-45 and 50-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 7-05)   Office Action Summary   Part of Paper No./Mail Date 060516

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/07/06 has been entered.

2. Applicant amended claims 1, 13, 30 and 37-38 has cancelled claims 46-49 and added new claims 50-53.

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

4. Applicant's arguments have been carefully considered but they were not found persuasive.

5. Applicant states that a supplemental Application Data Sheet was submitted on August 8, 2005 to change the Attorney Docket Number. The examiner acknowledges the receipt of the documents on the date indicated by applicant.

6. In the Remarks Applicant argues newly introduced claim limitations. In particular applicant argues that the art of record does not teach "an entity external to the interconnection system receiving a signal indicating detection of an attempted inter-node communication involving the at least one service component" and "in response

to receiving the signal the external entity providing at least a portion of the access control logic to the interconnection system".

7. The examiner respectfully disagrees. Both references used in the previous Final Office Action are directed towards firewalls that filter traffic. The newly introduced and argued limitations are at least implicit if not inherent. For example, in Fig. 1 *Dowd et al. (U.S. Patent No. 6141755)* shows an example of a firewall architecture, comprising several external (to each other) components. As it is clear from the figure there must be at least network input/output components (22, 26) a filtering component (24) a controller (28) and rule (ACL) database (30). Also, in computing systems any of the component must be alerted to events that the components must act upon. For example, IRQs calls or other signals are used for inter computing communication. As a result for the firewall to operate correctly there must be signals alerting to attempted inter-node communication that must be monitored/filtered and there and to retrieve appropriate logic from the firewall rule (ACL) database.

8. Unlike the previous claim limitations claims 50-53 comprise non standard or anticipated firewall features. However, applicant does not argue the limitation of these claims. As a result these limitations are addressed in this Office Action, below.

9. Claims 1-24, 26-28, 30-38, 42-45 and 50-53 have been examined.

Drawings

10. The amended claims including the new limitations such as "an entity external to the interconnection system and communicatively linked with the interconnection system ... programming the external entity with the access control logic ..." received and amendments to the specification received on 3/07/06 has been accepted. However, the drawings do not clearly disclose the limitations found in the newly amended claim language and the specification. As a result he drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the entity external to the interconnection system and programmed with the ACL must be shown or the feature(s) canceled from the claim(s). <u>No new matter should be entered.</u>

11. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the

changes are not accepted by the examiner, the applicant will be notified and

informed of any required corrective action in the next Office action. The objection to

the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

12. Claims 50-53 are rejected under 35 U.S.C. 112, second paragraph, as failing to set

forth the subject matter which applicant(s) regard as their invention.

13. The claims limitations recite:

"assigning to each application component a respective trustworthiness measure and

a respective criticality measure ...,

> wherein

the **trustworthiness** measure for each service component represents *an*

assessment of a potential threat the service component poses to other

objects,

> and wherein

the **criticality** measure for each service component represents a measure

selected from the group consisting of (i) a measure of importance of the service

component, and (ii) *a measure of concern for what the service component*

may do to other service components".

From the claim language it is not clear how trustworthiness differ from the

criticality measures since both measures seem to be concern with assessment of

a potential attack by the service components.

Claim Rejections - 35 USC § 102 or 103

14. Claims 1, 13 and 37 are rejected under 35 U.S.C. 102(b) as being anticipated by or,

in the alternative, under 35 U.S.C. 103(a) as obvious over *Pfleeger (Charles P.*

Pfleeger, "Security in Computing", ISBN 0133374866, 1996) as illustrated by *Dowd*

et al. (U.S. Patent 6141755).

As per claims 1 and 13 Pfleeger teaches a screening router that can allow or restrict

inter-node communication based on network addresses and port numbers (Pfleeger

sec. 9.5 pg. 426-428).

Providing at least a portion of the access-control logic to the interconnection system

in response to an attempted inter-node communication involving the at last one

service component is inherent. The main purpose of the firewalls (screening

routers) is to allow or block inter-node communication and inter-node

communications inherently involve multiple service components. As a result

Pfleeger's teaches a screening router implementing a company's policies that

screens communication allowing only the communication addressed to certain

addresses *(Pfleeger, Screening Router, pg. 429-430. The examiner points out that*

although Pfleeger discuses Screening Router firewall type, the whole Firewall

introduction pg. 426-428 is also relevant to applicant's limitations). This reads on

"providing at least a portion of the access-control logic to an interconnection system

in response to an attempted inter-node communication involving the at least one

service component (or between service components)" and "providing to the

interconnection system, in response to an attempted inter-node communication

between the application components, at least a portion of access-control rules that

define allowed communication between the application components".

15. *Pfleeger* does not explicitly teach an entity external to the interconnection system

and communicatively linked with the interconnection system programmed with the

access-control logic, and that the external entity responsively providing at least a

portion of the access-control logic to the interconnection system upon receiving the

signal indication detection of the attempted inter-node communication.

However, the limitation is at least implicit: a firewall able to filter traffic between

nodes must have at least some input/output mechanism, a flow switch, some control

mechanism such as a communication *(session)* manager and some firewall

database that stores firewall rules. *Dowd et al.* illustrate these separate *(external to*

each other) components in Fig. 1 and further discusses the figure in col. 5 line 65-

col. 6 line 30. The examiner also points out that in computer devices the events,

requests and responses are communicated using signal *(e.g. IRQ)*. As a result in

order for the firewall to act upon inter-node communication the session manager

must receive a signal that prompts the session manager to signal the database in

order to retrieve the corresponding rules.

16. Claims 1-8, 12-21, 24, 26, 31-32, 34, 36-38, 43 and 46-49 are rejected under 35

U.S.C. 102(e) as being anticipated by or, in the alternative, under 35 U.S.C. 103(a)

as obvious over *Wiegel (U.S. Patent No. 6484261)* as illustrated by *Dowd et al. (U.S.*

Patent 6141755).

As per claims 1, 13, 37 and 38 *Wiegel* teaches a method for controlling a network device that passes or rejects information messages, the method comprising the computer-implemented steps of defining a set of symbols that identify logical operations that can be carried out by the network device; defining an information communication policy for the network device by graphically interconnecting one or more of the symbols into a symbolic representation of the policy; and generating a set of instructions based on the symbolic representation of the policy, wherein the set of instructions causes the network device to selectively pass or reject messages according to the policy *(Wiegel, col. 5 lines 12-23)*.

Wiegel's invention is essentially an interface to a data communication filtering mechanism (firewall) that is used by the mechanism to filter data pockets based on the assigned rules *(Wiegel, col. 2 lines 36-65, col. 4 lines 24-33, col. 11 lines 30-42)*. Thus, *Weigel's* teaching reads on establishing access control logic restricting inter-node communication involving the at least one service component based on the identity of at least one of the service components, applying the access-control logic to block an inter-node communication involving the at least one service component and on providing to the interconnection system, in response to an attempted inter-node communication between the application components, at least a portion of access-control rules that define allowed communication between the application components.

17. *Wiegel* does not explicitly teach an entity external to the interconnection system and communicatively linked with the interconnection system programmed with the

access-control logic, and that the external entity responsively providing at least a

portion of the access-control logic to the interconnection system upon receiving the

signal indication detection of the attempted inter-node communication.

However, the limitation is at least implicit: rules restricting inter-node communication

taught by *Wiegel* are executed by a firewall, and firewalls capable to filter traffic

between nodes must have at least some input/output mechanism, a flow switch,

some control mechanism such as a communication *(session)* manager and some

firewall database that stores firewall rules. *Dowd et al.* illustrate these separate

(external to each other) components in Fig. 1 and further discusses the figure in col.

5 line 65-col. 6 line 30. The examiner also points out that in computer devices the

events, requests and responses are communicated using signal *(e.g. IRQ)*. As a

result in order for the firewall to act upon inter-node communication the session

manager must receive a signal that prompts the session manager to signal the

database in order to retrieve the corresponding rules.

18. As per claims 2-8, 12, 14-21, 24, 26, 28, 30-32, 34, 36, 38 and 46-48 *Wiegel*

teaches that sites determine how security policies are applied, how networks are

organized, and how network address translation works between two or more sites.

How a network packet travels across two sites determines which security polices are

applied. This traversal identifies the source and destination of the packet, thus

identifying the point of origin as one site. Security policies that are applied to a

particular site are enforced against all network packets that originate from that site

(col. 13 lines 14-22, col. 7 lines 45-54). *Wiegel's* invention utilizes applications, IP

addresses and ports related to source and destinations *(col. 7 lines 45-54)* and

applies the controls to Internet communication *(col. 10 lines 44-67)*. The system

comprises a firewall, a router and a switch that enforce one or more network security

policies and a policy translation agent responsible for translating or converting

policies as represented in knowledge base into a form that can be understood by a

firewall, a router or a switch *(Fig. 2, col. 11 lines 22-42)*. *Wiegel's* implementation is

associated with session operations, e.g. evaluates session requests *(col. 17 line 58-*

col. 18 line 40). Before policies are implemented to allow or disallow interconnection

system data flow they must be implemented on the computer that will implement the

policies. Also, computers inherently utilize interrupt signals during computer

operations, e.g. in order to switch from one task to another.

Claim Rejections - 35 USC § 103

19. Claims 9-11, 27, 33, 35, 42 and 44-45 are rejected under 35 U.S.C. 103(a) as being

unpatentable over *Wiegel (U.S. Patent No. 6484261)* in view of *Official Notice.*

20. As per claim 9 *Wiegel* does not explicitly teach that at least two processing nodes of

the plurality of interconnected processing nodes run different operating systems.

Official Notice is taken that it is old and well-known practice to interconnect

processing nodes running different operating systems.

It would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to interconnect processing nodes running different operating systems.

One of ordinary skill in the art at the time of applicant's invention would have been

motivated to utilize *Wiegel's* invention in the environment where interconnected

processing nodes run different operating systems for the benefit of interoperability.

21. Claims 10 and 44-45 are substantially equivalent to claim 9; therefore claims 10 and

44-45 are similarly rejected.

22. As per claims 11, 33 and 42 *Wiegel* does not explicitly teach that the computing

environment is a cluster-based computing environment.

Official Notice is taken that utilizing a cluster-based computing environment is old

and well-known practice.

It would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to utilize *Wiegel's* invention in a cluster-based computing environment.

One of ordinary skill in the art at the time of applicant's invention would have been

motivated to employ a cluster-based computing environment to take advantage of

communication accessibility.

23. As per claim 35 *Wiegel* does not teach an attempted inter-node communication

comprising an attempted inter-node between antagonistic service components and

application providers competing for business. Official notice is taken that it is old

and well-known in the art that the Internet includes nodes with antagonistic service

components hosted by many competing application providers. Thus, it is unrealistic

to keep all of the nodes with antagonistic services out of the Internet connection.

Therefore it would have been obvious that antagonistic serviced components would

have competed.

24. As per claim 27 *Wiegel* teaches that the switch utilizes a policy translation agent to translate or to convert policies as represented in knowledge base into a form that can be understood by the switch. *Wiegel* does not explicitly teach the switch translating the instructions by itself.

Official Notice is taken that it is old and well-known practice to implement instruction translation on a device that implements the instruction.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement instruction translation on a device that implements the instruction. One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ translation of the instruction on the executing device in order to speed up the execution process.

25. *Wiegel* also does not teach that the switch can receive command-line instructions. Official Notice is taken that it is old and well-known practice to provide computers with command line instructions that are interpreted/executed by the computers. One of ordinary skill in the art at the time of applicant's invention would have been motivated to employ command-line instructions to take advantage of quick access to and configuration of the switch.

26. Claims 50-53 are rejected under 35 U.S.C. 103(a) as obvious over *Pfleeger (Charles P. Pfleeger, "Security in Computing", ISBN 0133374866, 1996)* as illustrated by *Dowd et al. (U.S. Patent 6141755)* in view of *TCSEC (Department of Defense, "Trusted Computer System Evaluation Criteria", Dec 85)* and *Austel et al. (U.S. Patent No. 6430561).*

Pfleeger's teaching has been discussed above.

Pfleeger does not teach assigning to each service component a respective trustworthiness measure and a respective criticality measure, using the trustworthiness and criticality measures of each service component to select the at least a respective one of the processing nodes onto which each service component should be programmed, and programming each service component onto the at least a respective one of the processing nodes selected for the service component, wherein the trustworthiness measure for each service component represents an assessment of a potential threat the service component poses to other objects, and wherein the criticality measure for each service component represents a measure selected from the group consisting of (i) a measure of importance of the service component, and (ii) a measure of concern for what the service component may do to other service components.

TCSEC teaches assigning to each service component a respective trustworthiness measure and a respective criticality measure, using the trustworthiness and criticality measures of each service component, wherein the trustworthiness measure for each service component represents an assessment of a potential threat the service component poses to other objects, and wherein the criticality measure for each service component represents a measure selected from the group consisting of (i) a measure of importance of the service component, and (ii) a measure of concern for what the service component may do to other service components *(TCSEC, pg. 2, 10, Appendix B etc.)*.

It would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to assigning to each service component a respective trustworthiness

measure and a respective criticality measure, using the trustworthiness and criticality

measures of each service component to select the at least a respective one of the

processing nodes onto which each service component should be programmed, and

programming each service component onto the at least a respective one of the

processing nodes selected for the service component, wherein the trustworthiness

measure for each service component represents an assessment of a potential threat

the service component poses to other objects, and wherein the criticality measure

for each service component represents a measure selected from the group

consisting of (i) a measure of importance of the service component, and (ii) a

measure of concern for what the service component may do to other service

components as taught by *TCSEC* giving the benefit of providing basis for specifying

security requirements and standards for systems satisfying sensitivity requirements.

TCSEC does not explicitly teach considering trustworthiness measure and a

respective criticality measure levels in selecting processing nodes onto which each

service component should be programmed. However, the limitation is implicit. As it

is shown by *Austel et al.* in col. 1 and 2, for example, special measures *(e.g.*

mandatory access controls) have been devised to deal with non trusted software

and it would have been obvious to one of ordinary skill in the art at the time of

applicant's invention to select nodes with appropriate functionalities to complement

the level of trustworthiness criticality of respective service components that would be

programmed into the node given the benefit of integrity, reliability and availability.

27. Claims 50-53 are rejected under 35 U.S.C. 103(a) as obvious over *Wiegel (U.S.*

Patent No. 6484261) as illustrated by *Dowd et al. (U.S. Patent 6141755)* in view of

TCSEC (Department of Defense, "Trusted Computer System Evaluation Criteria",

Dec 85) and *Austel et al. (U.S. Patent No. 6430561).*

Wiegel teaching has been discussed above.

Wiegel does not teach assigning to each service component a respective

trustworthiness measure and a respective criticality measure, using the

trustworthiness and criticality measures of each service component to select the at

least a respective one of the processing nodes onto which each service component

should be programmed, and programming each service component onto the at least

a respective one of the processing nodes selected for the service component,

wherein the trustworthiness measure for each service component represents an

assessment of a potential threat the service component poses to other objects, and

wherein the criticality measure for each service component represents a measure

selected from the group consisting of (i) a measure of importance of the service

component, and (ii) a measure of concern for what the service component may do to

other service components.

TCSEC teaches assigning to each service component a respective trustworthiness

measure and a respective criticality measure, using the trustworthiness and criticality

measures of each service component, wherein the trustworthiness measure for each

service component represents an assessment of a potential threat the service

component poses to other objects, and wherein the criticality measure for each

service component represents a measure selected from the group consisting of (i) a

measure of importance of the service component, and (ii) a measure of concern for

what the service component may do to other service components *(TCSEC, pg. 2,*

10, Appendix B etc.).

It would have been obvious to one of ordinary skill in the art at the time of applicant's

invention to assigning to each service component a respective trustworthiness

measure and a respective criticality measure, using the trustworthiness and criticality

measures of each service component to select the at least a respective one of the

processing nodes onto which each service component should be programmed, and

programming each service component onto the at least a respective one of the

processing nodes selected for the service component, wherein the trustworthiness

measure for each service component represents an assessment of a potential threat

the service component poses to other objects, and wherein the criticality measure

for each service component represents a measure selected from the group

consisting of (i) a measure of importance of the service component, and (ii) a

measure of concern for what the service component may do to other service

components as taught by *TCSEC* giving the benefit of providing basis for specifying

security requirements and standards for systems satisfying sensitivity requirements.

28. *TCSEC* does not explicitly teach considering trustworthiness measure and a

respective criticality measure levels in selecting processing nodes onto which each

service component should be programmed. However, the limitation is implicit. As it

is shown by *Austel et al.* in col. 1 and 2, for example, special measures *(e.g.*

mandatory access controls) have been devised to deal with non trusted software

and it would have been obvious to one of ordinary skill in the art at the time of

applicant's invention to select nodes with appropriate functionalities to complement

the level of trustworthiness criticality of respective service components that would be

programmed into the node given the benefit of integrity, reliability and availability.
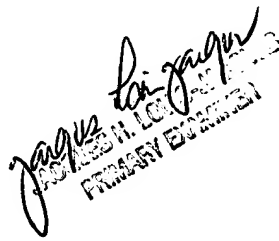
Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Peter Poltorak whose telephone number is (571)

272-3840. The examiner can normally be reached Monday through Thursday from

9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Jacques Louis Jacques can be reached on (571)272-6962. The fax

phone number for the organization where this application or proceeding is assigned

is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).